

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-287192

(43)Date of publication of application : 13.10.2000

(51)Int.Cl.

H04N 7/167

G09C 1/00

H04L 9/08

H04L 9/32

H04L 12/56

(21)Application number : 11-093916

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 31.03.1999

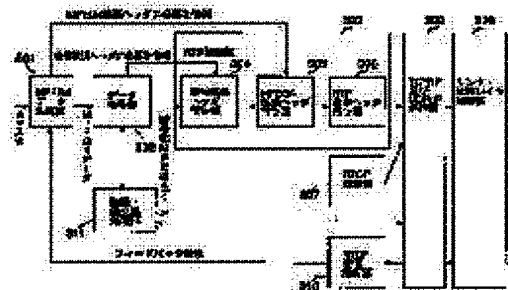
(72)Inventor : SAITO TAKESHI
KATO HIROSHI
TOMOTA ICHIRO
TAKAHATA YOSHIAKI
AMI JUNKO

(54) INFORMATION DISTRIBUTING DEVICE, RECEIVING DEVICE AND COMMUNICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To extend copy protection technique to a digital contents circulation by executing a transport protocol processing required for transferring contents information, creating a basic transport header which indicates that contents information is enciphered and transmitting a packet including desired information to a communication opposite party by way of a network.

SOLUTION: MPEG4 data outputted from an MPEG4 data creating part 301 are enciphered by a data enciphering part 302. An authentication and key exchange processing part 311 generates a new cipher key for an enciphering processing in the case of the updating timing of the cipher key and gives it to the data enciphering part 302. Together with it, the value of information to be a source for generating a common key is increased and given to the part 302. The value of information to be the source for generating the common key is given from the part 302 to a cipher extension header giving part 304. An MPEG4 extending header is exempted from a ciphering object.



(19)日本特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2000-287192
(P2000-287192A)

(43)公開日 平成12年10月13日(2000.10.13)

(51)Int.Cl. ⁷	識別記号	F I	ページ・ド(参考)
H 0 4 N 7/167		H 0 4 N 7/167	Z 5 C 0 6 4
G 0 9 C 1/00	6 4 0	C 0 9 C 1/00	6 4 0 Z 5 J 1 0 4
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 C 5 K 0 3 0
9/32			6 Y 5 A 9 A 0 0 1
12/56		11/20	1 0 2 F
審査請求 未請求 請求項の数15 O L (全 25 頁)			

(21)出願番号 特願平11-93918

(22)出願日 平成11年3月31日(1999.3.31)

(71)出願人 000003078

株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者 斉藤 健

神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

(73)発明者 加藤 拓

東京都府中市東芝町1番地 株式会社東芝
府中工場内

(74)代理人 100058479

弁理士 鈴木 武彦 (外6名)

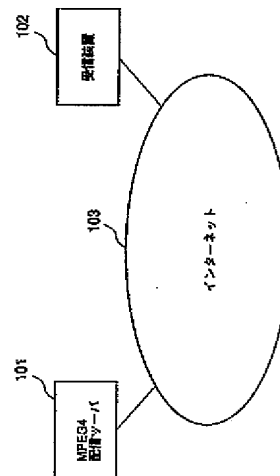
最終頁に続く

(54)【発明の名称】 情報配信装置、受信装置及び通信方法

(57)【要約】

【課題】 コピープロテクション技術を I E E E 1 3 9 4 のみならずインターネット上のコンテンツ流通にも拡張可能な情報配信装置を提供すること。

【解決手段】 コンテンツを暗号化してインターネット経由で受信装置に配信する配信装置であって、受信装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行ない、所定の符号化方式で符号化されたコンテンツを暗号化し、転送されるコンテンツが暗号化されたものであるか否かを示す属性情報および該コンテンツの暗号方式を示す属性情報のうちの少なくとも一方の属性情報を含む暗号化に関する属性情報からなる暗号拡張ヘッダを作成し、コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、基本トランスポートヘッダを作成し、基本トランスポートヘッダと暗号拡張ヘッダと暗号化されたコンテンツ情報とを含むパケットを送出する。



【特許請求の範囲】

【請求項1】コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、前記通信相手装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行なう手段と、所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、前記暗号化に関する属性情報および前記符号化方式を示す情報を含む暗号拡張ヘッダを作成する手段と、前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、転送されるコンテンツ情報が暗号化されたものである旨を示す情報を含む基本トランスポートヘッダを作成する手段と、前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出する手段とを備えたことを特徴とする情報配信装置。

【請求項2】コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、前記通信相手装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行なう手段と、所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、前記暗号化に関する属性情報を含む暗号拡張ヘッダを作成する手段と、前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、転送されるコンテンツ情報が暗号化されたものである旨および該コンテンツ情報の符号化方式を示す情報を含む基本トランスポートヘッダを作成する手段と、前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出する手段とを備えたことを特徴とする情報配信装置。

【請求項3】コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、前記通信相手装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行なう手段と、所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、前記暗号化に関する属性情報を含む暗号拡張ヘッダを作成する手段と、前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、基本トランスポートヘッダを作成する手段と、前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前

記ネットワーク経由で前記通信相手装置に送出する手段とを備え、前記基本トランスポートヘッダには、少なくとも転送されるコンテンツ情報が暗号化された可能性を有するものである旨を示す情報を記述し、前記暗号拡張ヘッダには、少なくとも転送されるコンテンツ情報が暗号化されたものであるか否かを示す情報を記述し、前記基本トランスポートヘッダまたは前記暗号拡張ヘッダには、前記コンテンツ情報の符号化方式を示す情報をも記述することを特徴とする情報配信装置。

【請求項4】コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、前記通信相手装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行なう手段と、所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、前記暗号化に関する属性情報を含む暗号拡張ヘッダを作成する手段と、前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、基本トランスポートヘッダを作成する手段と、前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出する手段とを備え、前記暗号拡張ヘッダには、転送されるコンテンツ情報が暗号化されたものであるか否かを示す情報および転送されるコンテンツ情報の暗号方式を示す情報のうちの少なくとも一方を記述することを特徴とする情報配信装置。

【請求項5】前記暗号拡張ヘッダを前記パケットのパケットヘッダ内の拡張ヘッダとすることを特徴とする請求項1ないし4のいずれか1項に記載の情報配信装置。

【請求項6】前記暗号拡張ヘッダを前記パケットのペイロード内のペイロードヘッダとすることを特徴とする請求項1ないし4のいずれか1項に記載の情報配信装置。

【請求項7】前記コンテンツ情報の属性情報を含むコンテンツ拡張ヘッダを作成する手段を更に備え、前記コンテンツ拡張ヘッダを前記パケットのペイロード内のペイロードヘッダとすることを特徴とする請求項1ないし6のいずれか1項に記載の情報配信装置。

【請求項8】前記コンテンツ拡張ヘッダは暗号化しないことを特徴とする請求項7に記載の情報配信装置。

【請求項9】所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置であって、前記情報配信装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行なう手段と、前記認証処理の後に前記情報配信装置から、基本トラン

スポーツヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信する手段と、
前記基本トランスポートヘッダにより前記コンテンツ情報が暗号化されたものであることが示されている場合、前記暗号拡張ヘッダに含まれる前記暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号する手段とを備えたことを特徴とする情報受信装置。
【請求項10】所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置であって、前記情報配信装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行なう手段と、前記認証処理の後に前記情報配信装置から、基本トランスポートヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信する手段と、前記基本トランスポートヘッダにより前記コンテンツ情報が暗号化されたものであることが示されている場合、該暗号拡張ヘッダに含まれる暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号する手段とを備えたことを特徴とする情報受信装置。
【請求項11】前記基本トランスポートヘッダまたは前記暗号拡張ヘッダを参照して前記コンテンツ情報の符号化方式を調べる手段を更に備えたことを特徴とする請求項9または10に記載の情報受信装置。
【請求項12】所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置であって、前記情報配信装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行なう手段と、前記認証処理の後に前記情報配信装置から、基本トランスポートヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信する手段と、前記暗号拡張ヘッダにより前記コンテンツ情報が暗号化されたものであることが示されている場合、該暗号拡張ヘッダに含まれる暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号する手段とを備えたことを特徴とする情報受信装置。
【請求項13】受信した前記基本トランスポートヘッダを参照して一定以上の遅延時間または一定以上のパケット廃棄が確認された場合に、前記情報配信装置に対して所定の暗号化パラメータの送信を要求する手段を更に備えたことを特徴とする請求項9ないし12のいずれか1項に記載の情報受信装置。
【請求項14】コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置の通信方法であって、前記通信相手装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行ない、

所定の符号化方式で符号化されたコンテンツ情報を暗号化し、
転送されるコンテンツ情報が暗号化されたものであるか否かを示す属性情報および該コンテンツ情報の暗号方式を示す属性情報のうちの少なくとも一方の属性情報を含む前記暗号化に関する属性情報からなる暗号拡張ヘッダを作成し、
前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、基本トランスポートヘッダを作成し、
前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出することを特徴とする通信方法。
【請求項15】所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置の通信方法であって、前記情報配信装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行ない、前記認証処理の後に前記情報配信装置から、基本トランスポートヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信し、
前記暗号拡張ヘッダにより前記コンテンツ情報が暗号化されたものであることが示されている場合、該暗号拡張ヘッダに含まれる暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号することを特徴とする通信方法。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、インターネット等のネットワークを介したデータ送受信を著作権保護を考慮して行う情報配信装置、受信装置及び通信方法に関する。
【0002】
【従来の技術】近年、デジタル放送の開始や、デジタルAV機器の発売等、いわゆる「家庭AV環境のデジタル化」が大きな注目を集めている。デジタルAVデータは、様々な圧縮が可能、マルチメディアデータとしての処理が可能、何回再生しても劣化が無い、等の優れた特徴を持ち、今後その用途はますます広がっていくものと考えられる。
【0003】しかしながらその反面、このデジタルAV技術には、「コンテンツの不正コピーを容易に行うことができる」という側面もある。すなわち、どのようなデジタルコンテンツについても、原理的に「ビットのコピー」で、元通りの品質でしかも恒久的に劣化の無い複製が作成されてしまうため、いわゆる「不正コピー」の問題が発生する。
【0004】そこで、この「不正コピー」を防ぐための技術が種々検討されている。その中の一つが、CPTW

G (コピープロテクション技術ワーキンググループ) で検討されている「1394CPコンテンツ保護システム仕様(1394CP Content Protection System Specification)」である。この技術は、IEEE1394バスに接続されたノード間で、転送するコンテンツ(例えばMPEGデータ等)について、送受信ノードの間で予め認証手続きをおこない、暗号鍵(コンテンツキー)を共有できるようにしておき、以降はそのコンテンツをその暗号鍵で暗号化して転送し、認証手続きを行った両ノード以外のノードにはそのコンテンツが復号化できないようにする技術である。このようにすることにより、認証を行っていないノードは、暗号鍵の値がわからないため、転送されているデータ(すなわち暗号化されたコンテンツデータ)をたとえ取り込むことができたとしても、このデータを復号化することはできない。このような認証に参加できるノードを、あらかじめ定められた認証機関が許可したノードのみとしておくことで、不正なノードが暗号鍵を入手することを未然に防ぎ、コンテンツの不正コピーを予め防ぐことが可能になる。

【0005】

【発明が解決しようとする課題】さて、デジタルコンテンツの流通は、当然ながらIEEE1394上に限定されるものではなく、ネットワーク一般に対して期待されるのではなく、公衆網や、物理/リンクネットワークにとらわれない技術インフラとして、インターネットは、その有力な候補となろう。

【0006】しかしながら、現在はインターネット上のデジタルコンテンツ(特にデジタルAVストリーム)の流通は、著作権保護のなされないまま、生のデータのままでRTP(リアルタイムトランスポートプロトコル)上を転送される方式が主流となっている。

【0007】本発明は、上記事情を考慮してなされたもので、コピープロテクション技術をIEEE1394のみならずインターネット等のネットワーク上のデジタルコンテンツ流通にも拡張することの可能な情報配信装置、受信装置及び通信方法を提供することを目的とする。

【0008】

【課題を解決するための手段】本発明(請求項1)は、コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、前記通信相手装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行なう手段と、所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、前記暗号化に関する属性情報および前記符号化方式を示す情報を含む暗号拡張ヘッダを作成する手段と、前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、転送されるコンテンツ情報が暗号化されたもの

である旨を示す情報を含む基本トランスポートヘッダを作成する手段と、前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出する手段とを備えたことを特徴とする。

【0009】本発明(請求項2)は、コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、前記通信相手装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行なう手段と、所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、前記暗号化に関する属性情報を含む暗号拡張ヘッダを作成する手段と、前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、転送されるコンテンツ情報が暗号化されたものである旨および該コンテンツ情報の符号化方式を示す情報を含む基本トランスポートヘッダを作成する手段と、前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出する手段とを備えたことを特徴とする。

【0010】本発明(請求項3)は、コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、前記通信相手装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行なう手段と、所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、前記暗号化に関する属性情報を含む暗号拡張ヘッダを作成する手段と、前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、基本トランスポートヘッダを作成する手段と、前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出する手段とを備え、前記基本トランスポートヘッダには、少なくとも転送されるコンテンツ情報が暗号化された可能性を有するものである旨を示す情報を記述し、前記暗号拡張ヘッダには、少なくとも転送されるコンテンツ情報が暗号化されたものであるか否かを示す情報を記述し、前記基本トランスポートヘッダまたは前記暗号拡張ヘッダには、前記コンテンツ情報の符号化方式を示す情報をも記述することを特徴とする。

【0011】本発明(請求項4)は、コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置であって、前記通信相手装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行なう手段と、所定の符号化方式で符号化されたコンテンツ情報を暗号化する手段と、前記暗号化に関する属性情報を含む暗号拡張ヘッダを作成する手段と、前記コンテンツ

情報の転送に必要なトランスポートプロトコル処理を行うとともに、基本トランスポートヘッダを作成する手段と、前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出する手段とを備え、前記暗号拡張ヘッダには、転送されるコンテンツ情報が暗号化されたものであるか否かを示す情報および転送されるコンテンツ情報の暗号方式を示す情報のうちの少なくとも一方を記述することを特徴とする。

【0012】好ましくは、前記暗号拡張ヘッダには、転送されるコンテンツ情報の符号化方式を示す情報をも記述するようにしてもよい。

【0013】好ましくは、前記暗号拡張ヘッダを前記パケットのパケットヘッダ内の拡張ヘッダとするようにしてもよい。

【0014】好ましくは、前記暗号拡張ヘッダを前記パケットのペイロード内のペイロードヘッダとするようにしてもよい。

【0015】好ましくは、前記コンテンツ情報の属性情報を含むコンテンツ拡張ヘッダを作成する手段を更に備え、前記コンテンツ拡張ヘッダを前記パケットのペイロード内のペイロードヘッダとするようにしてもよい。

【0016】好ましくは、前記コンテンツ拡張ヘッダは暗号化しないようにしてもよい。

【0017】本発明（請求項9）は、所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置であって、前記情報配信装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行なう手段と、前記認証処理の後に前記情報配信装置から、基本トランスポートヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信する手段と、前記基本トランスポートヘッダにより前記コンテンツ情報が暗号化されたものであることが示されている場合、前記暗号拡張ヘッダに含まれる前記暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号する手段とを備えたことを特徴とする。

【0018】本発明（請求項10）は、所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置であって、前記情報配信装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行なう手段と、前記認証処理の後に前記情報配信装置から、基本トランスポートヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信する手段と、前記基本トランスポートヘッダにより前記コンテンツ情報が暗号化された可能性を有するものであることが示されている場合、前記暗号拡張ヘッダを参照して暗号化の有無を調べ、暗号化されたものであるならば、該暗号拡張ヘッダに含ま

れる暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号する手段とを備えたことを特徴とする。

【0019】好ましくは、前記基本トランスポートヘッダまたは前記暗号拡張ヘッダを参照して前記コンテンツ情報の符号化方式を調べる手段を更に備えるようにしてもよい。

【0020】本発明（請求項12）は、所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置であって、前記情報配信装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行なう手段と、前記認証処理の後に前記情報配信装置から、基本トランスポートヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信する手段と、前記暗号拡張ヘッダにより前記コンテンツ情報が暗号化されたものであることが示されている場合、該暗号拡張ヘッダに含まれる暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号する手段とを備えたことを特徴とする。

【0021】好ましくは、受信した前記基本トランスポートヘッダを参照して一定以上の遅延時間または一定以上のパケット廃棄が確認された場合に、前記情報配信装置に対して所定の暗号化パラメータの送信を要求する手段を更に備えるようにしてもよい。

【0022】本発明（請求項14）は、コンテンツ情報を暗号化して所定のトランスポートプロトコルによるネットワーク経由で通信相手装置に配信する情報配信装置の通信方法であって、前記通信相手装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行ない、所定の符号化方式で符号化されたコンテンツ情報を暗号化し、転送されるコンテンツ情報が暗号化されたものであるか否かを示す属性情報および該コンテンツ情報の暗号方式を示す属性情報のうちの少なくとも一方の属性情報を含む前記暗号化に関する属性情報からなる暗号拡張ヘッダを作成し、前記コンテンツ情報の転送に必要なトランスポートプロトコル処理を行うとともに、基本トランスポートヘッダを作成し、前記基本トランスポートヘッダと前記暗号拡張ヘッダと前記暗号化されたコンテンツ情報とを含むパケットを前記ネットワーク経由で前記通信相手装置に送出することを特徴とする。

【0023】本発明（請求項15）は、所定のトランスポートプロトコルによるネットワーク上の情報配信装置からコンテンツ情報の配信を受ける情報受信装置の通信方法であって、前記情報配信装置との間で認証手続きおよび認証鍵交換手続きの少なくとも一方を含む認証処理を行ない、前記認証処理の後に前記情報配信装置から、基本トランスポートヘッダと、暗号拡張ヘッダ、コンテンツ情報とを含むパケットを受信し、前記暗号拡張ヘッダ

により前記コンテンツ情報が暗号化されたものであることが示されている場合、該暗号拡張ヘッダに含まれる暗号化に関する属性情報に基づいて、該暗号化されたコンテンツ情報を復号することとを特徴とする。

【0024】本発明によれば、送信側において、RTP（リアルタイムトランスポートプロトコル）やHTTP（ハイパーテキストトランスファープロトコル）トランスポートプロトコルにおける拡張ヘッダあるいはペイロードヘッダの形で、暗号拡張ヘッダを設け、該暗号拡張ヘッダに暗号化に関する属性情報（例えば、暗号化の有無、暗号方式、コピー属性に関する情報（暗号モードインジケータ）、コンテンツキー（共通鍵）を生成するものとなる情報（Even/Oddフィールド）、等）を記述することにより、送信側から受信側に安全にコンテンツデータを転送し、また受信側においてペイロードにて転送される暗号化されたコンテンツデータを復号することができる。

【0025】また、従来のRTPでは、そのペイロードタイプフィールドに、「ペイロードに格納されているデータの符号化方式」が記載されているのみで、ペイロードに格納されているデータが、（ネットワークレイヤや、トランスポートレイヤではなくて）コンテンツレイヤにて暗号化されていた場合に、これを相手側装置に通知する方法がなかったが、本発明によれば、RTPのペイロードタイプフィールドに「暗号化データ」あるいは「暗号化された特定の符号化方式で符号化されたデータ」である旨を記述できるため、これを相手側装置に通知することができるようになり、もって、前述の暗号化されたコンテンツの送受が行えるようになる。

【0026】このように本発明によれば、AVストリーム伝送のコピープロテクション技術をIEEE1394のみならずインターネット等のネットワーク上のデジタルコンテンツ流通にも拡張するが可能となる。

【0027】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【0028】また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0029】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【0030】（第1の実施形態）図1に、本実施形態における情報配信システムの構成例を示す。図1では、インターネット103に本実施形態に係るMPEG4配信サーバ101および受信装置102が接続されており、

インターネット103を通してMPEG4配信サーバ101と受信装置102との間でMPEG4のAVストリームの秘匿通信を行うものである。もちろん、インターネット103には他のMPEG4配信サーバや受信装置あるいはその他の種類の機器が接続されていてもかまわない。

【0031】また、本実施形態では、データの種別をMPEG4として説明するが、もちろん他の種類のデータにも本発明は適用可能である。

【0032】このMPEG4配信サーバ101は、受信装置102に対して、MPEG4データの配信を行う。MPEG4データは、ファイル転送の形ではなく、ストリーム配信の形をとる。このとき、著作権保護の対象とするMPEG4データは、暗号化した状態で配信する。その際、配信に先立って、MPEG4配信サーバ101と受信装置102との間で、認証手続きや認証鍵の交換の手続きなどを行う。

【0033】このときのシーケンスの一例を図2に示す。

【0034】なお、図2は、いわゆるコンテンツレイヤの暗号化や認証について示したものであり、IPレイヤあるいはトランスポートレイヤ等のレイヤにおけるセキュリティやそれらレイヤでの認証手続き等に関しては省略しており、またコンテンツレイヤで先立って行われる課金などの手続きも省略してある（課金処理や他レイヤの認証/暗号処理が行われない場合もあり得る）。

【0035】ここでは、受信装置102がMPEG4配信サーバ101に対して配信の要求を行う場合を考える。この場合は、最初の認証要求は受信装置102から送出される（S201）。認証要求では、その機器（受信装置102）が予め定められた認証機関から「著作権保護を受けたコンテンツのやりとりを行うことのできる機器である」との証明を受けている証書（certificate、機器証明）の交換も同時に行ってもよい。

【0036】ここで、機器証明の際に用いる「機器のID」は、IPアドレスを使用してもよいが、IPアドレスはDHCPサーバなどで与えられる場合には、装置のブート毎に可変の値になってしまう可能性がある。そこで、機器証明で使われる機器IDとしては、その装置のMACアドレス、あるいはEUI64アドレス、あるいはそれらのアドレスに部品モジュール番号を付与したものなどを利用してもよい。また、その装置のCPUの識別番号や、MPEG4デコーダの識別番号等、（理想的には）世界唯一であると考えられる数値（あるいは、その地域で唯一、等、同一な値がほとんど期待されない数値）を、「機器のID」として用いてもよい。

【0037】受信装置102からのメッセージを受信したMPEG4配信サーバ101は、認証要求の応答と、証書（機器証明）の交換を行う（S202）。

【0038】次に、MPEG4配信サーバ101および

受信装置102は、共通の認証鍵を生成するために、認証鍵の生成プロセスを行う(S203)。この手続きの詳細については、例えばIEEE1394のコピープロテクションの認証鍵の生成プロセスと同様のものであってもよい。このプロセスが終了すると、MPEG4配信サーバ101および受信装置102は共通の認証鍵 K_{auth} を、第三者に知られることなく、共有することができる。

【0039】次に、MPEG4配信サーバ101は、交換鍵 K_x と認証鍵 K_{auth} との排他的論理和($K_x \oplus K_{auth}$)と乱数 N_c を受信装置102に送信する(S204、S205)。受信装置102では、受信した($K_{auth} \oplus K_x$)の値と(K_{auth})の値との排他的論理和を計算して($K_x \oplus K_{auth} \oplus K_{auth} = K_x$)、交換鍵 K_x を取り出す。

【0040】この時点で、MPEG4配信サーバ101および受信装置102は、認証鍵 K_{auth} 、交換鍵 K_x 、乱数 N_c という3種類の数値を共有していることになる。

【0041】ここで、暗号鍵(コンテンツキー) K_c 、すなわちMPEG4配信サーバ101が送信すべきMPEG4データを暗号化するための暗号鍵であって且つ受信装置102が受信した暗号化されたMPEG4データを復号化するための暗号鍵(共有鍵) K_c は、MPEG4配信サーバ101および受信装置102の各々において、予め定められた同一の関数 J を用いることにより、上記の数値の一部の関数として算出される。例えば、 $K_c = J[K_x, f(EMI), N_c]$ と算出される。ここで、EMIとは、「そのデータ(コンテンツ)のコピー属性」を意味し、「そのデータは無制限にコピー可能であるか、それとも1回だけコピー可能であるか、それとも2回だけコピー可能であるか、それとも無条件にコピー不可であるか、コピー済みでこれ以上コピー不可であるか、…」等の属性をあらわす。この属性値EMIはある特定の関数 f で変換したものが $f(EMI)$ である。これらの関数 J や f は、外部に対して秘密であってもよい。

【0042】さて、暗号鍵 K_c が生成された後、MPEG4配信サーバ101は、この暗号鍵 K_c でコンテンツ(MPEG4データ)を暗号化して、インターネット上に転送する(S206、S207、…)。

【0043】なお、後述するように、暗号化コンテンツは「AVストリームデータのリアルタイム転送」の形を取りつつインターネット上に転送されるため、トランスポートプロトコルとしてはRTP(リアルタイムトランスポートプロトコル)が採用される。

【0044】また、この暗号鍵 K_c は時変にする(すなわち、ある時間が経過すると値が変わる)。例えば、前回の変更時から所定の時間(所定の時間は、一定でもよ

いし、可変でもよい)が経過したことが認識された場合には、変数 N_c の値をインクリメントし、再度、上記の関数 J を用いて暗号鍵 K_c の値を計算する。このとき、暗号化 K_c の値を更新するタイミング(あるいはどのデータから使用する暗号鍵 K_c を更新するか)を送受信側で同期して認識する必要がある。このため、転送されるMPEG4データ(AVデータ)に、Even/Oddフィールドなる領域を設け、このフィールドの値の変わりを、変数 N_c の値、ひいては暗号鍵 K_c の値の変わりを規定する(当該データから更新後の暗号鍵 K_c が適用される)。

【0045】すなわち、MPEG4配信サーバ101では上記時間の経過を監視し、暗号鍵 K_c を更新するタイミングになったことが検出された場合、変数 N_c の値をインクリメントして暗号鍵 K_c の値を計算し直し、この再計算後の暗号鍵 K_c を使用して送信すべきMPEG4データを暗号化するとともに、Even/Oddフィールドの値をインクリメントさせて、送信を行う。以降は、次の更新タイミングまで、この暗号鍵 K_c を使用して暗号化を行う。一方、受信装置102では、受信したEven/Oddフィールドの値を監視し、その値が直前に受信した値に比較してインクリメントされていることが検出された場合、変数 N_c の値をインクリメントして暗号鍵 K_c の値を計算し直し、この再計算後の暗号鍵 K_c を使用して受信した暗号化データを復号化する。以降、次にEven/Oddフィールドの値の変化が検出されるまで、この暗号鍵 K_c を使用して復号化を行う。

【0046】このようにして、MPEG4配信サーバ101と受信装置102間で暗号化されたMPEG4データのやり取りがなされる。

【0047】図3に、MPEG4配信サーバ101の内部構成例を示す。

【0048】図3に示されるように、本実施形態のMPEG4配信サーバ101は、MPEG4データ生成部301、データ暗号部302、暗号拡張ヘッダ付与部304とMPEG4拡張ヘッダ付与部305とRTP基本ヘッダ付与部306を含み、RTPの処理を行うRTP処理部303、RTP送信部307、TCP/IP及びUDP/IP処理部308、リンク・物理レイヤ処理部309、RTP受信解析部310、認証・鍵交換処理部311を備えている。

【0049】図2のシーケンスの認証や暗号に関する処理(S201～S205までの処理)および暗号鍵更新に関する処理は、認証・鍵交換処理部311により行われる。

【0050】さて、入力されたAV入力(例えばアナログ信号)は、MPEG4データ生成部301にてMPEG4のデータに圧縮される。

【0051】このとき、「どこがIピクチャか」、「符号化レートはいくらか」等、生成しているMPEG4に

ついで属性情報をMPEG4データ転送時に同時に受信側に通知すると、受信側においてその再生(復号)処理が行いやすくなる場合がある。特にインターネットでは、転送するパケットの廃棄、遅延、到着順の変更等が起こり得るため、それらの属性情報を得ることは、受信側で高品質に再生するためには欠かせない情報である。例えば、本実施形態のMPEG4の場合であれば、VO Pヘッダに関する情報等がこれにあたる。また、MPEG4システムに関わる情報、例えば、Sync Layerによる同期情報の伝達や、複数MPEG4ストリームを多重化して送信する場合の多重化のための情報あるいはオブジェクトディスクリプタの初期値や最新値に関する情報等が必要な場合も考えられる。このため、AVデータをRTPにて転送する場合には、RTPの拡張ヘッダまたはRTPペイロードのペイロードヘッダという形で、送信するAVデータと並行して属性情報を送ることが行われる。

【0052】本実施形態では、これらの属性情報がRTP拡張ヘッダの形で送信されるものとする。すなわち、「MPEG4拡張ヘッダ」なる種別(ID)のRTP拡張ヘッダとして送信される。このため、MPEG4データ生成部301からMPEG4拡張ヘッダ付与部305に対して必要な情報が通知される。

【0053】次に、MPEG4データ生成部301から出力されたMPEG4データをデータ暗号部302が暗号化する。その際に使用する暗号鍵は、前述の時変の暗号鍵Kcである。また、この暗号処理についても、種々の属性情報が考えられ、本実施形態では「暗号拡張ヘッダ」なる種別(ID)のRTP拡張ヘッダが暗号拡張ヘッダ付与部304にて付与される。このため、データ暗号部302から暗号拡張ヘッダ付与部304に対して必要な情報が通知される。

【0054】なお、上記の暗号処理のために、認証・鍵交換処理部311では、暗号鍵Kcの更新のタイミングになった場合には、Ncをインクリメントして前述の関数Jにより新たな暗号鍵Kcを生成してデータ暗号部302に渡す。また、これとともに、前述のEven/Oddフィールドの値をインクリメントして、データ暗号部302に渡す。Even/Oddフィールドの値は、上記のようにデータ暗号部302から暗号拡張ヘッダ付与部304に渡される。

【0055】ここで、図4に、暗号拡張ヘッダの一例を示す。図4に示されるように、この暗号拡張ヘッダには、拡張ヘッダ種別フィールド、暗号化有無フィールド、暗号方式表示フィールド、暗号モードインジゲータ(EMI)フィールド、Even/Oddフィールドがある。拡張ヘッダ種別フィールドは、当該拡張ヘッダの種別を示す情報を記述するためのフィールドである。この場合、拡張ヘッダ種別フィールドには暗号拡張ヘッダを示す情報が記述される。暗号化有無フィールドは、当

該RTPパケットで転送されるデータが暗号化されたものであるか否かを示す情報を記述するためのフィールドである。暗号方式表示フィールドは、当該RTPパケットで転送されるデータに対して使用する暗号方式を示す情報を記述するためのフィールドである。例えば、暗号方式がM6であることを示す情報が記述される。暗号モードインジゲータ(EMI)フィールドは、前述のコピー属性値EMIを記述するためのフィールドである。Even/Oddフィールドは、前述した通り、送信側から受信側に対して暗号鍵の更新タイミングを通知するためのフィールドである。

【0056】なお、ここでは、各フィールドは一例として8ビットとしているが、これに限定されるものではなく、適宜定めることが可能である。

【0057】ここで、あるAVデータを暗号化して受信側に送ると、早送り等のトリックプレイを行ったりあるいは部分的な静止画像を送ったりしたいときなどに受信側での処理が困難になる場合がある。これは、暗号化されたAVストリームの内の一部分だけを送信するという作業に困難を伴うからである(例えば、Ncの値がインクリメントではなく、いくつかに飛んでしまう、等の理由による)。このため特定の場合に受信側に対してAVデータに暗号をかけずに送信したいという場合が考えられる。この場合、受信側に対して「このAVデータには暗号をかけています/いません」といった情報を通知する機構が必要となる。上記の暗号化有無フィールドは例えばこの目的で使われる。

【0058】また、「あるストリームについてはこの暗号方式、別のあるストリームについてはこの暗号方式」といったように、インターネット上では、異なる暗号方式が共存する可能性がある。このような場合、「このAVデータは、どの暗号方式で暗号化されているか」を示すフィールドがあると、受信側では、このフィールドを見て、適当な復号化エンジンを選択して、暗号を復号化することができるようになる。上記の暗号方式表示フィールドは例えばこの目的で使われる。

【0059】また、図4に示すように、暗号モードインジゲータ(EMI)フィールドには、IEEE1394の場合の2ビットと異なり、8ビット用意してある。これは、「このAVデータはN回までコピー可能」という情報を通知するときにそのNの数値の選択に自由度を持たせることや、特殊なコピーを認める場合(例えば、ある条件が満たされているときに限りコピーを可能とする場合)などに、このフィールドの値が多くの値を取れるようにしておくことで、それらに対応できるようにするためである。

【0060】また、図4に示すように、Even/Oddフィールドには、IEEE1394の場合と1ビットと異なり、8ビット用意してある。これは、前述のようにインターネットではパケットの廃棄、遅延、到着順の

逆転が起こり得ることから、1ビットの情報量では充分ではないとの配慮からである。すなわち、例えばインターネットではS207に示すようなEven/Oddビット=1のパケットがすべて廃棄されるような場合が想定し得る。この場合、Even/Oddフィールドを1ビットとすると、次のパケットではEven/Oddビットは0に戻ってしまうため、受信側から見ると「Even/Oddビットが0である状態が継続されている(Even/Oddビットに変化はない)」と認識されてしまう。このように、実際にはNcは2つインクリメントされるべきであるのに、Even/Oddビットの値が変わっていないと認識されることで、Ncの値のインクリメントがなされず、正しい暗号鍵の生成ができない、という問題点が発生し得る。そこで、Even/Oddフィールドには、2ビット以上、例えば8ビット用意し、インターネットにおけるパケット廃棄/遅延/到着順逆転が起こっても、受信側が適切な処理ができるように配慮してある。

【0061】ここで、本実施形態においては、データの暗号化は、MPEG4データそのものに対してのみ行われ、MPEG4拡張ヘッダに対しては行われない。MPEG4拡張ヘッダは、いわゆる「著作権を守るべきコンテンツ」ではなく、受信側にてMPEG4データそのものを使用するのに先立って使用されるものであるため、これは暗号化の対象から外している。

【0062】結局、RTP処理部303では、暗号拡張ヘッダ付与部304にて暗号拡張ヘッダが、MPEG4拡張ヘッダ付与部305にてMPEG4拡張ヘッダが、RTP基本ヘッダ付与部306にてRTP基本ヘッダが、それぞれ付与され、図5に示すような形のRTPヘッダが付与されることになる。ここで、暗号拡張ヘッダはデータ暗号部302からの情報に基づいて生成され、MPEG4拡張ヘッダはMPEG4データ生成部301からの情報に基づいて生成される。また、RTPヘッダは、タイムスタンプやシーケンス番号など、インターネット上をAVデータを転送する場合に必要な基本的なパラメータを要素として持つ(なお、詳細は例えばRFC1889に開示されている)。

【0063】RTPヘッダが付与された(暗号化された)MPEG4データは、TCP/IP及びUDP/IP処理部308にて図6のようなIPパケットとして、リンク・物理レイヤ処理部309を通してインターネット103に送出される。

【0064】図7に、受信装置102の内部構成例を示す。

【0065】図7に示されるように、本実施形態のMPEG4配信サーバ101は、リンク・物理レイヤ処理部701、TCP/IP及びUDP/IP処理部702、RTP基本ヘッダ受信解析部704とMPEG4拡張ヘッダ受信解析部705と暗号拡張ヘッダ受信解析部70

6を含み、RTPの処理を行うRTP処理部703、データ暗号復号部707、MPEG4データデコード部708、受信状態解析部709、RTCP送信部710、認証・鍵交換処理部711を備えている。

【0066】図2のシーケンスの認証や暗号に関する処理(S201～S205までの処理)および暗号鍵更新に関する処理は、認証・鍵交換処理部711により行われる。

【0067】さて、受信装置102は、基本的には、MPEG4配信サーバ101の逆順に逆変換の処理を行なう。

【0068】すなわち、まず、インターネット103を介して転送されてきたMPEG4データ(RTPヘッダが付与された暗号化データ)は、リンク・物理レイヤ処理部701からTCP/IP及びUDP/IP処理部702を経て、RTP処理部703に入力される。

【0069】RTP処理部303では、RTP基本ヘッダ受信解析部704にてRTP基本ヘッダが解析され、MPEG4拡張ヘッダ受信解析部705にてMPEG4拡張ヘッダが解析され、暗号拡張ヘッダ受信解析部304にて暗号拡張ヘッダが解析される。また、MPEG4拡張ヘッダ受信解析部705からMPEG4データデコード部708に対して必要な情報が通知され、暗号拡張ヘッダ受信解析部304からデータ暗号復号部707に対して必要な情報が通知される。

【0070】そして、RTPペイロードの暗号化データは、RTP処理部703からデータ暗号復号部707に渡される。データ暗号復号部707は、暗号拡張ヘッダ受信解析部304からの情報に基づいて復号を行う(暗号を解く)。

【0071】その際に使用する暗号鍵は、前述の時変の暗号鍵Kcである。すなわち、データ暗号復号部707は、暗号拡張ヘッダ受信解析部304から通知された暗号拡張ヘッダの暗号化有無フィールドの値を参照することにより受信データが暗号化されていることが分かり(この結果、復号を行うことが決定され)、次にEven/Oddフィールドを参照し、その値を直前に受信した値と比較することによって、インクリメントされている場合には、暗号鍵を更新することが分かる(同一である場合には、暗号鍵は更新されないことになる)。そして、暗号鍵を更新する旨をデータ暗号復号部707から認証・鍵交換処理部711に伝え、認証・鍵交換処理部711では、暗号鍵Kcの更新のタイミングになったので、Ncをインクリメントして前述の関数Jにより新たな暗号鍵Kcを生成してデータ暗号復号部707に渡す。

【0072】さらに、復号化された(暗号の解かれた)MPEG4データはデータ暗号復号部707からMPEG4データデコード部708に渡され、MPEG4データデコード部708は、MPEG4拡張ヘッダ受信解析

部705からの情報に基づいて該MPEG4データをデコードし、AV出力（例えばアナログ信号）として出力する。

【0073】ところで、RTPにはRTCP（リアルタイムトランスポート制御プロトコル）なるプロトコルが付随している。このRTCPは、RTPのシーケンス番号やタイムスタンプ等を監視し、受信側（本実施形態の場合受信装置102）から送信側（本実施形態の場合、MPEG4配信サーバ101）に対して、受信状況（パケット廃棄率、パケット配送遅延時間等）を通知する機能がある。これを行なうのが受信装置102の受信状態解析部709とRTCP送信部710である。MPEG4配信サーバ101は、このRTCPパケットを、RTCP受信解析部310で受信し、必要に応じてMPEG4データ生成部301にフィードバックをして、最適化を図ることができる。例えば、パケット廃棄が激しい場合は、ネットワークが混雑していると考えて、MPEG4データ生成のビットレートを下げる等のフィードバック制御を行なうようにしてもよい。なお、MPEG4配信サーバ101のRTCP送信部307は、RTCPに必要な情報を送信する。

【0074】さて、前述のように、受信装置102では、受信したパケットの暗号拡張ヘッダに含まれるEven/Oddフィールドの監視結果に基づいて、暗号鍵Kcの計算に用いる変数Ncの値を変更する。したがって、送信側から受信側に確実にNcの値を更新した旨を伝えることができないと、受信側で暗号鍵Kcの値が計算できないことになり、送信されてくる暗号化データの復号ができないことになる。

【0075】インターネットは基本的にパケットの廃棄が起こり得るネットワークであるため、Even/Oddフィールドの値の意味（インクリメントのタイミング）が正確に通信相手に伝わる保証は無い（特に、Even/Oddフィールドのビット長が短いとき）。そこで、受信装置102は、「正確なNcの値を知りたい」と考えた場合に、送信装置（本実施形態の場合、MPEG4配信サーバ101）に対して、Ncの値を要求するオプションを用意するようにしてもよい。

【0076】ここで、受信装置102が「正確なNcの値を知りたい」と考える場合の例としては、RTP基本ヘッダのタイムスタンプ、あるいはシーケンス番号等で、想定以上に値の「飛び」があった場合に、Ncの値を要求するパケットを送信側に送出する、という方式が考えられる。この「想定値以上の値の飛び」は、「その間にEven/Oddビットの値が変化した可能性がある」ということにつながるためである。これらの処理を行なうのは、MPEG4配信サーバ101または受信装置102の認証・鍵交換処理部である。このようにすることにより、もし仮にMPEG4配信サーバ101と受信装置102との間でEven/Oddビットの同期が

外れてしまった場合でも、適切な復帰処理を行なうことができるようになる。なお、MPEG4配信サーバ101から受信装置102にNcの値を通知する場合は、対応するRTPや拡張ヘッダ、ペイロードヘッダ等のタイムスタンプやシーケンス番号等の値も同時に通知するようにしてもよい。

【0077】また、配信されたデータを受信装置（あるいは、受信装置に装着された、DVD-RAM等の何らかのストレージメディア）に蓄積する場合も考えられる。この場合は、配信されたデータを、暗号化されたデータのままで、対応する暗号鍵Kcとともに蓄積するようにしてもよい。

【0078】（第2の実施形態）次に、第1の実施形態のパケット形式のバリエーションとなる第2の実施形態について説明する。本実施形態は基本的な構成や動作においては第1の実施形態と同様であるので、本実施形態では第1の実施形態と相違する点を中心に説明する。

【0079】本実施形態が第1の実施形態と相違する点は、第1の実施形態ではRTPヘッダの拡張ヘッダとして、「暗号拡張ヘッダ」と「MPEG4拡張ヘッダ」を付加したが（図5、図6参照）、本実施形態では、「暗号拡張ヘッダ」はRTPヘッダの拡張ヘッダとして付加するが、「MPEG4拡張ヘッダ」はRTPのペイロードにペイロードヘッダとして搭載する点である（図9、図10参照）。

【0080】本実施形態のネットワークの全体構成は第1の実施形態（図1）と同様である。また、処理のシーケンスも第1の実施形態（図2）と同様である。また、暗号拡張ヘッダも第1の実施形態（図4）と同様である。

【0081】図8に、本実施形態のMPEG4配信サーバ101の構成例を示す。本実施形態では、MPEG4拡張ヘッダをRTPのペイロードにペイロードヘッダとして搭載するので、MPEG4拡張ヘッダの処理がRTP処理外となり、図3のMPEG4拡張ヘッダ付与部305がRTP処理部303内から外へ出され、MPEG4ペイロードヘッダ付与部315となっている点が第1の実施形態と相違する点である。

【0082】図9に、本実施形態において暗号化されたAVデータの送信の際に用いられるRTPヘッダの形式を示す。ここで、本実施形態では、RTP基本ヘッダには「当該RTPパケットで転送されるデータの属性（符号化方式等）」を示す「ペイロードタイプ」というフィールドを設けている。本実施形態では、例えば転送されるデータが暗号化されたMPEG4である場合に、このフィールドには「暗号化されたMPEG4」を示す情報が記述される。受信装置102は、このフィールドを参照することにより、転送されているデータが暗号化されたMPEG4であることを知ることができる。また、本実施形態では、RTP基本ヘッダには「当該RTPヘッ

ダには、拡張ヘッダが付加されているか否か」を示す「Xビット」というフィールドを設けている。本実施形態では、「拡張ヘッダあり」を示すビットが立つことになる。

【0083】図10に、本実施形態において、インターネット上を転送されるIPパケット全体の形式を示す。

【0084】図11に、本実施形態の受信装置102の構成例を示す。上記のMPEG4配信サーバ101と同様に、MPEG4拡張ヘッダの処理がRTP処理外となり、図7のMPEG4拡張ヘッダ受信解析部705がRTP処理部703内から外へ出され、MPEG4ペイロードヘッダ受信解析部715となっている点が第1の実施形態と相違する点である。

【0085】受信装置102では、RTP基本ヘッダ受信解析部704にて、受信したデータが暗号化されたMPEG4であることが分かり、また、RTPヘッダに拡張ヘッダが付加されていることが分かる。そして、暗号拡張ヘッダ受信解析部706にて、その拡張ヘッダが暗号拡張ヘッダであることが分かり、また、暗号拡張ヘッダから暗号方式や暗号鍵の更新の有無等を知ることができる。そして、第1の実施形態と同様にデータ暗号復号部707にて暗号化MPEG4データを復号し、MPEG4ペイロードヘッダ受信解析部715にてMPEG4ペイロードヘッダを解析し、さらに第1の実施形態と同様にMPEG4データ生成部708にて上記解析結果に基づいてMPEG4データをデコードして、AV出力（例えばアナログ信号）として出力する。

【0086】なお、本実施形態においては、ペイロードタイプフィールドに暗号化有りの通知を含む情報が記述されている場合には暗号拡張ヘッダの暗号化有無フィールドを参照しないようにしてもよいし、ペイロードタイプフィールドに暗号化有りの通知を含む情報が記述されている場合に、それは暗号化されている可能性のある旨の通知であるものとして、暗号拡張ヘッダの暗号化有無フィールドによって最終的な暗号化の有無を決定するようにしてもよい。

【0087】（第3の実施形態）次に第3の実施形態について説明する。本実施形態では、第2の実施形態と相違する点を中心に説明する。

【0088】図12に、本実施形態において暗号化されたAVデータの送信の際に用いられるRTPヘッダの形式を示す。また、図13に、本実施形態において、インターネット上を転送されるIPパケット全体の形式を示す。

【0089】すなわち、第2の実施形態では、RTP基本ヘッダ内のペイロードタイプフィールドに、「暗号化されたMPEG4」というように、暗号化の有無もしくは暗号化の可能性の有無の通知を含む情報を記述したが、本実施形態では、「MPEG4」のみを記述し、ペイロードタイプフィールドには、暗号化の有無もしくは

暗号化の可能性の有無の通知を含む情報は記述しない。

【0090】従って、本実施形態では、受信装置102は、ペイロードタイプフィールドを参照することにより、受信データがMPEG4であることを知ることができるが、暗号化の有無については、RTPヘッダのRTP拡張ヘッダ（暗号拡張ヘッダ）を参照して認識することになる。

【0091】受信装置102では、RTP基本ヘッダ受信解析部704にて、受信したデータがMPEG4であることが分かり、また、RTPヘッダに拡張ヘッダが付加されていることが分かる。そして、暗号拡張ヘッダ受信解析部706にて、その拡張ヘッダが暗号拡張ヘッダであることが分かり、また、暗号拡張ヘッダから暗号化の有無や暗号鍵の更新の有無等を知ることができる。以降は、第2の実施形態と同様である。

【0092】（第4の実施形態）次に第4の実施形態について説明する。本実施形態では、第2の実施形態と相違する点を中心に説明する。

【0093】本実施形態が第2の実施形態と相違する点は、第2の実施形態では「暗号拡張ヘッダ」はRTPヘッダの拡張ヘッダとして付加し、「MPEG4拡張ヘッダ」はRTPのペイロードにペイロードヘッダとして搭載するが（図9、図10参照）、本実施形態では、「暗号拡張ヘッダ」と「MPEG4拡張ヘッダ」の両方をRTPのペイロードにペイロードヘッダとして搭載する点である（図15、図16参照）。

【0094】本実施形態のネットワークの全体構成は第2（第1）の実施形態（図1）と同様である。また、処理のシーケンスも第2（第1）の実施形態（図2）と同様である。また、暗号拡張ヘッダ（暗号ペイロードヘッダ）も第2（第1）の実施形態（図4）と同様である。

【0095】図14に、本実施形態のMPEG4配信サーバ101の構成例を示す。本実施形態では、MPEG4拡張ヘッダに加えて暗号拡張ヘッダをもRTPのペイロードにペイロードヘッダとして搭載するので、暗号拡張ヘッダの処理がRTP処理外となり、図8の暗号拡張ヘッダ付与部304もRTP処理部303内から外へ出され、暗号ペイロードヘッダ付与部314となっている点が第2の実施形態と相違する点である。

【0096】図15に、本実施形態において暗号化されたAVデータの送信の際に用いられるRTPヘッダの形式を示す。ペイロードタイプフィールドについては第2の実施形態と同様である。また、Xビットフィールドについてはその役割は第2の実施形態と同様であるが、本実施形態では、「拡張ヘッダなし」を示すビットが立つことになる。

【0097】図16に、本実施形態において、インターネット上を転送されるIPパケット全体の形式を示す。

【0098】図17に、本実施形態の受信装置102の構成例を示す。上記のMPEG4配信サーバ101と同

様に、暗号拡張ヘッダの処理がRTP処理外となり、図11の暗号拡張ヘッダ受信解析部706がRTP処理部703内から外へ出され、暗号ペイロードヘッダ受信解析部716となっている点が第2の実施形態と相違する点である。

【0099】受信装置102では、RTP基本ヘッダ受信解析部704にて、受信したデータが暗号化されたMPEG4であることが分かり、また、RTPヘッダに拡張ヘッダが付加されていないことが分かる。本実施形態では、以降は、ペイロードに対する処理になる。まず、暗号ペイロード受信解析部716にて、そのペイロードヘッダが暗号拡張ヘッダであることが分かり、また、暗号ペイロードヘッダから暗号方式や暗号鍵の更新の有無等を知ることができる。そして、以降は第2の実施形態と同様に、データ暗号復号部707にて暗号化MPEG4データを復号し、MPEG4ペイロードヘッダ受信解析部715にてMPEG4ペイロードヘッダを解析し、さらにMPEG4データ生成部708にて上記解析結果に基づいてMPEG4データをデコードして、AV出力（例えばアナログ信号）として出力する。

【0100】なお、本実施形態においても第2の実施形態と同様に、ペイロードタイプフィールドに暗号化有りの通知を含む情報が記述されている場合には暗号ペイロードヘッダの暗号化有無フィールドを参照しないようにしてもよいし、ペイロードタイプフィールドに暗号化有りの通知を含む情報が記述されている場合に、それは暗号化されている可能性のある旨の通知であるものとして、暗号ペイロードヘッダの暗号化有無フィールドによって最終的な暗号化の有無を決定するようにしてもよい。

【0101】（第5の実施形態）次に第5の実施形態について説明する。本実施形態では、第2の実施形態と相違する点を中心に説明する。

【0102】図18に、本実施形態において暗号化されたAVデータの送信の際に用いられるRTPヘッダの形式を示す。また、図19に、本実施形態における暗号拡張ヘッダの形式を示す。また、図20に、本実施形態において、インターネット上で転送されるIPパケット全体の形式を示す。

【0103】すなわち、第2の実施形態では、RTP基本ヘッダ内のペイロードタイプフィールドに、「暗号化されたMPEG4」というように、その暗号化データの属性（符号化方式等）の通知を含む情報を記述したが（図9、図11参照）、本実施形態では、「暗号化データ」というように、ペイロードタイプフィールドには、「暗号化データ」という暗号化有りを通知する情報のみを記述する（図18、図20参照）。そして、暗号拡張ヘッダをRTPヘッダの拡張ヘッダとして付加し、MPEG4拡張ヘッダをRTPのペイロードにペイロードヘッダとして搭載する点は第2の実施形態と同様である

が、本実施形態では、上記の暗号化データの属性（符号化方式等）については暗号拡張ヘッダ内に記述するようにしている（図4、図19参照）。

【0104】本実施形態のネットワークの全体構成は第2（第1）の実施形態（図1）と同様である。また、処理のシーケンスも第2（第1）の実施形態（図2）と同様である。また、MPEG4配信サーバおよび受信装置102の内部構造も第2の実施形態（図8、図11）と同様である。

【0105】図18に示すように、本実施形態では、RTP基本ヘッダのペイロードタイプフィールドには「暗号化されたデータ」を示す値が記述される。受信装置102は、このフィールドを参照することにより、転送されているデータが暗号化されたデータであることを知ることができる。また、本実施形態では、Xビットフィールドには「拡張ヘッダあり」を示すビットが立つことになる。

【0106】図19に示すように、本実施形態では、暗号拡張ヘッダには、ペイロードタイプフィールドを設ける。ペイロードタイプフィールドには、ペイロードに入るデータの種別（本実施形態の場合、MPEG4）を示す情報が記述される。受信装置102は、このフィールドを参照することにより、転送されているデータの種別を知ることができる。

【0107】受信装置102では、RTP基本ヘッダ受信解析部704にて、受信したデータが暗号化されたデータであることが分かり、また、RTPヘッダに拡張ヘッダが付加されていることが分かる。そして、暗号拡張ヘッダ受信解析部706にて、その拡張ヘッダが暗号拡張ヘッダであることが分かり、また、暗号拡張ヘッダから暗号方式や暗号鍵の更新の有無等およびペイロードに入るデータの種別を知ることができる。そして、第2の実施形態と同様に、データ暗号復号部707にて暗号化MPEG4データを復号し、MPEG4ペイロードヘッダ受信解析部715にてMPEG4ペイロードヘッダを解析し、さらにMPEG4データ生成部708にて上記解析結果に基づいてMPEG4データをデコードして、AV出力（例えばアナログ信号）として出力する。

【0108】なお、本実施形態においても第2の実施形態と同様に、RTP基本ヘッダのペイロードタイプフィールドに暗号化データを示す情報が記述されている場合には暗号拡張ヘッダの暗号化有無フィールドを参照しないようにしてもよいし、RTP基本ヘッダのペイロードタイプフィールドに暗号化データを示す情報が記述されている場合に、それは暗号化されている可能性のある旨の通知であるものとして、暗号拡張ヘッダの暗号化有無フィールドによって最終的な暗号化の有無を決定するようにしてもよい。

【0109】（第6の実施形態）次に第6の実施形態について説明する。本実施形態では、第4の実施形態と相

達する点を中心に説明する。

【0110】図21に、本実施形態において暗号化されたAVデータの送信の際に用いられるRTPヘッダの形式を示す。また、本実施形態における暗号拡張ヘッダの形式は図19と同様である。また、図22に、本実施形態において、インターネット上に転送されるIPパケット全体の形式を示す。

【0111】すなわち、「暗号拡張ヘッダ」と「MPEG4拡張ヘッダ」の両方をRTPのペイロードにペイロードヘッダとして搭載する点は第4の実施形態と同様であるが(図15、図16参照)、第4の実施形態では、RTP基本ヘッダ内のペイロードタイプフィールドに、「暗号化されたMPEG4」というように、その暗号化データの属性(符号化方式等)の通知を含む情報を記述するのに対し、本実施形態では、「暗号化データ」というように、ペイロードタイプフィールドには、「暗号化データ」という暗号化有りを通知する情報のみを記述する(図21、図22参照)。そして、暗号拡張ヘッダをRTPヘッダの拡張ヘッダとして付加し、MPEG4拡張ヘッダをRTPのペイロードにペイロードヘッダとして搭載する点は第2の実施形態と同様であるが、本実施形態では、上記の暗号化データの属性(符号化方式等)については暗号拡張ヘッダ内に記述するようにしている(図4、図19参照)。

【0112】本実施形態のネットワークの全体構成は第4(第1)の実施形態(図1)と同様である。また、処理のシーケンスも第4(第1)の実施形態(図2)と同様である。また、MPEG4配信サーバおよび受信装置102の内部構造も第4の実施形態(図14、図17)と同様である。

【0113】図21に示されるように、本実施形態では、RTP基本ヘッダのペイロードタイプフィールドには「暗号化されたデータ」を示す値が入る。受信装置102は、このフィールドを見ることにより、転送されているデータが暗号化されたものであることを知ることができる。また、Xビットには「拡張ヘッダ無し」を示すビットが立つ。また、第4の実施形態と同様に、暗号拡張ヘッダのペイロードタイプフィールドに、ペイロードに入るデータの種別(本実施形態の場合、MPEG4)を示す情報が記述される。

【0114】受信装置102では、RTP基本ヘッダ受信解析部704にて、受信したデータが暗号化されたデータであることが分かり、また、RTPヘッダに拡張ヘッダが付加されていないことが分かる。本実施形態では、以降は、ペイロードに対する処理になる。まず、暗号ペイロード受信解析部716にて、そのペイロードヘッダが暗号拡張ヘッダであることが分かり、また、暗号ペイロードヘッダから暗号方式や暗号鍵の更新の有無等およびペイロードに入るデータの種別を知ることができる。そして、以降は第4の実施形態と同様に、データ暗

号復号部707にて暗号化MPEG4データを復号し、MPEG4ペイロードヘッダ受信解析部715にてMPEG4ペイロードヘッダを解析し、さらにMPEG4データ生成部708にて上記解析結果に基づいてMPEG4データをデコードして、AV出力(例えばアナログ信号)として出力する。

【0115】なお、本実施形態においても第4の実施形態と同様に、RTP基本ヘッダのペイロードタイプフィールドに暗号化データを示す情報が記述されている場合には暗号拡張ヘッダの暗号化有無フィールドを参照しないようにしてもよいし、RTP基本ヘッダのペイロードタイプフィールドに暗号化データを示す情報が記述されている場合に、それは暗号化されている可能性のある旨の通知であるものとして、暗号拡張ヘッダの暗号化有無フィールドによって最終的な暗号化の有無を決定するようにしてもよい。

【0116】(第7の実施形態)第1～第6の実施形態では、本発明をトランスポートプロトコルとしてRTPを使用するシステムに適用した場合について説明してきたが、本発明は、それ以外のプロトコルを使用するシステムに対しても適用可能である。

【0117】第7の実施形態では、トランスポートプロトコルとしてRTPを使うのではなく、MPEG4のデータ配信を、WWWサーバとWebブラウザ間のプロトコルであるHTTP(ハイパーテキストトランスファープロトコル)(およびTCP)を使って行なう場合の例について説明する。

【0118】図23に、本実施形態における情報配信システムの構成例を示す。図23では、インターネット6103に本実施形態に係るMPEG4配信サーバ6101が接続され、LAN6105に本実施形態に係る受信装置6102が接続されており、LAN6105はプロキシサーバ6104を介してインターネット6103に接続されている。そして、受信装置6102は、LAN6105、プロキシサーバ6104、インターネット6103を介してMPEG4配信サーバ6101との間でMPEG4のAVストリームの秘密通信を行うものである。もちろん、インターネット6103には他のMPEG4配信サーバあるいはその他の種類の機器が接続されていてもかまわないし、LAN6106には他の受信装置あるいはその他の種類の機器が接続されていてもかまわない。

【0119】また、本実施形態では、データの種別をMPEG4として説明するが、もちろん他の種類のデータにも本発明は適用可能である。

【0120】さて、図23において、各々の装置はIPをサポートしている装置であるが、インターネット6103とLAN6105との間にHTTPプロキシサーバ6104が存在しているため、LAN6105上のIPアドレスは、グローバルIPアドレスであっても、プ

イベントIPアドレスであってもよい。ここで、プロキシサーバとは、インターネットとイントラネットの間に入り、HTTP（その他のプロトコルでもよい）を一度終端すると共に、プロキシサーバの両端のHTTPセッションを結び付けて、実質上受信装置（Webブラウザ）から要求のあったHTTPコンテンツを配信サーバ（WWWサーバ）に対して（あるいは逆方向に）データを配信できるようにするためのサーバである。なお、プロキシサーバの詳細については、例えばhttp://squid.nlanr.net/Squid/等に表示されている。本実施形態においては、MPEG4配信サーバはWWWサーバ、受信装置はWebブラウザであってもよい。

【0121】図24に、認証手続きや認証鍵の交換の手続きあるいは暗号化されたデータ等のシーケンスの一例を示す。受信装置6102とMPEG4配信サーバ6101との間にプロキシサーバ6102が入っているために実際のメッセージ（HTTPメッセージとして転送される）は一度プロキシサーバ6102にて中継される点がこれまでの第1～第6の実施形態（図2）と相違するだけであり、それ以外の点は第1～第6の実施形態と同様の手続きである。

【0122】さて、MPEG4配信サーバ6101、受信装置6102、パケットの形式などについては、例えば、前述した第1～第6の実施形態において対応するものについて、トランスポートプロトコルに依存する部分をHTTPプロトコルに対応するように修正すれば、HTTPプロトコルに対応したMPEG4配信サーバ6101、受信装置6102、パケットの形式などを構成することができる。以下では、「暗号拡張ヘッダ」は拡張ヘッダとして付加するが「MPEG4拡張ヘッダ」はペイロードにペイロードヘッダとして搭載する構成（第2の実施形態参照）に対応する構成を例にとって説明する。

【0123】図25に、MPEG4配信サーバ6101の内部構成例を示す。

【0124】図25に示されるように、本実施形態のMPEG4配信サーバ6101は、MPEG4データ生成部6301、データ暗号部6302、MPEG4ペイロードヘッダ付与部6305、暗号ヘッダ付与部6304とMIMEヘッダ付与部6306を含むHTTP処理部6303、TCP/IP及びUDP/IP処理部6308、リンク・物理レイヤ処理部6309、認証・鍵交換処理部6311を備えている。

【0125】図24のシーケンスの認証や暗号に関する処理（S6201～S6205までの処理）および暗号鍵更新に関する処理は、認証・鍵交換処理部6311により行われる。

【0126】HTTP処理部6303がこれまでの実施形態のRTP処理部に相当し、MIMEヘッダ付与部6

306がこれまでの実施形態のRTP基本ヘッダ付与部に相当する。

【0127】図26に、インターネット（及びLAN）上を転送されるIPパケットを示し、図27に、MIME基本ヘッダおよび暗号拡張ヘッダの詳細を示す。

【0128】本実施形態では、暗号拡張ヘッダは、MIMEの一つのパートとして転送される。このため、暗号拡張ヘッダは、MIMEの“Content-Type”に、それが暗号拡張ヘッダである旨を示す情報が記載される。また、MPEG4拡張ヘッダはペイロードヘッダとして暗号化されたMPEG4データとともにMIMEの一つのパートとして転送される。MPEG4拡張ヘッダの付加された暗号化MPEG4データは、MIMEの“Content-Type”に、それがMPEG4データである旨を示す情報が記載される。なお、MIMEの詳細については例えばRFC2045等に表示されている。

【0129】暗号拡張ヘッダの形式は、第1の実施形態と同様である。

【0130】図28に、受信装置6102の内部構成例を示す。

【0131】図28に示されるように、本実施形態のMPEG4配信サーバ6101は、リンク・物理レイヤ処理部6701、TCP/IP及びUDP/IP処理部6702、MIMEヘッダ解析部6704と暗号ヘッダ解析部6706を含むHTTP処理部6703、MPEG4ペイロードヘッダ解析部6705、データ暗号復号部6707、MPEG4データデコード部6708、認証・鍵交換処理部6711を備えている。

【0132】図24のシーケンスの認証や暗号に関する処理（S6201～S6205までの処理）および暗号鍵更新に関する処理は、認証・鍵交換処理部6711により行われる。

【0133】HTTP処理部6703がこれまでの実施形態のRTP処理部に相当し、MIMEヘッダ解析部6306がこれまでの実施形態のRTP基本ヘッダ受信解析部に相当する。

【0134】MPEG4配信サーバ6101においては、入力されたAV入力（例えばアナログ信号）は、MPEG4データ生成部6301にてMPEG4のデータに圧縮される。また、MPEG4データ生成部6301からMPEG4ペイロードヘッダ付与部6305に対して必要な情報が通知される。

【0135】次に、MPEG4データ生成部6301から出力されたMPEG4データをデータ暗号部6302が暗号化する。その際に使用する暗号鍵は、前述の時変の暗号鍵Kcである。また、データ暗号部6302から暗号ヘッダ付与部6304に対して必要な情報が通知される。

【0136】次に、HTTP処理部6303では、暗号

ヘッダ付与部6304にて暗号拡張ヘッダが付加され、MIMEヘッダ付与部6036にてMIMEヘッダが付加される。

【0137】そして、MIMEヘッダが付与された暗号化されたMPEG4データは、TCP/IP及びUDP/IP処理部6308にて図26のようなIPパケットとして、リンク・物理レイヤ処理部6309を通してインターネット6103に送出される。

【0138】受信装置6102においては、MIMEヘッダ解析部6704にて、受信したデータが暗号化された可能性のあるMPEG4であることが分り、また、MIMEの一つのパートとして暗号拡張ヘッダが付加されていることが分かる。そして、暗号ヘッダ解析部6706にて、その暗号拡張ヘッダから暗号化の有無、暗号方式や暗号鍵の更新の有無等を知ることができる。そして、第2の実施形態と同様に、データ暗号復号部6707にて暗号化MPEG4データを復号し、MPEG4ペイロードヘッダ解析部6715にてMPEG4ペイロードヘッダ（これまでの実施形態のMPEG4ペイロードヘッダと同様）を解析し、さらにMPEG4データ生成部6708にて上記解析結果に基づいてMPEG4データをデコードして、AV出力（例えばアナログ信号）として出力する。

【0139】なお、ここでは、「暗号拡張ヘッダ」は拡張ヘッダとして付加するが「MPEG4拡張ヘッダ」はペイロードにペイロードヘッダとして搭載する構成を示したが、例えば、「暗号拡張ヘッダ」および「MPEG4拡張ヘッダ」を拡張ヘッダとして付加する構成や、「暗号拡張ヘッダ」および「MPEG4拡張ヘッダ」をペイロードにペイロードヘッダとして搭載する構成など、他の構成も可能である。

【0140】ところで、第1～第7の実施形態では、送信側から受信側へ暗号鍵Kcの生成のための変数Ncの値の更新を通知するために、暗号拡張ヘッダ（暗号ペイロードヘッダ）のEven/Oddフィールドを用いたが、その代わりに、Ncの値を送信するようにしてもよい。この場合に、Ncの値は、1づつインクリメントするのではなく、その都度ランダムに発生するようにしてもよい。また、Ncの値をパケット毎に変化させるようにしてもよい。

【0141】また、第1～第7の実施形態では、転送プロトコルとしてRTPやH.264を用いてきたが、もちろんその他のプロトコルを用いてもよい。また、適用できるネットワークもインターネットに限定されるものではない。また、前述したように、転送するデータの種別もMPEG4に限定されるものではない。

【0142】また、第2、第3、第5の実施形態では、データ暗号部302/データ暗号復号部707をRTP処理部303、307の外部に設けたが、それらをRTP処理部303、307の内部に設けるようにしてもよ

い。

【0143】（第8の実施形態）次に第8の実施形態について説明する。

【0144】第1～第7の実施形態では、図2に例示したシーケンスを用いて説明したが、もちろん本発明は、その他のシーケンスについても適用可能である。

【0145】以下では、その他のシーケンスを用いた例について説明する。なお、ここでは、受信装置がMPEG4配信サーバから配信されたMPEG4データを蓄積する場合を考える。

【0146】本実施形態の情報配信システムの構成例は図1と同様とする。図1では、インターネット103に本実施形態に係るMPEG4配信サーバ101および受信装置102が接続されており、インターネット103を通してMPEG4配信サーバ101と受信装置102との間でMPEG4のAVストリームの秘密通信を行うものである。もちろん、インターネット103には他のMPEG4配信サーバや受信装置あるいはその他の種類の機器が接続されていてもかまわない。

【0147】また、本実施形態でもデータの種別をMPEG4として説明するが、もちろん他の種別のデータにも本発明は適用可能である。

【0148】このMPEG4配信サーバ101は、受信装置102に対して、MPEG4データの配信を行う。MPEG4データは、ファイル転送の形ではなく、ストリーム配信の形をとる。このとき、著作権保護の対象とするMPEG4データは、暗号化した状態で配信する。その際、配信に先立って、MPEG4配信サーバ101と受信装置102との間で、認証手続きや認証鍵の交換の手続きなどを行う。

【0149】このときのシーケンスの一例を図29に示す。

【0150】なお、図29は、いわゆるコンテンツレイヤの暗号化や認証について示したものであり、IPレイヤあるいはトランスポートレイヤ等のレイヤにおけるセキュリティやそれらレイヤでの認証手続き等に関しては省略してあり、またコンテンツレイヤで先立って行われる課金などの手続きも省略してある（課金処理や他レイヤでの認証/暗号処理が行われない場合もあり得る）。

【0151】第1の実施形態と同様に、MPEG4配信サーバ101と受信装置102は、認証と、証書（機器証明）の交換を行う（S7201、S7202）。

【0152】ここで、MPEG4配信サーバ101は、コンテンツ（送信するAVデータ）を復号するための暗号鍵Kcを受信装置102に通知する必要があるが、受信装置102にて無制限にコンテンツの不正コピーを行なうことができないように、以下のような方を請じる。すなわち、受信装置102のストレージメディア（例えばDVD-RAM）に記録するとき、AVデー

は暗号化された状態で記録する。また、そのストレージメディア上のデータを再生する場合も、それが本来そのストレージメディアに記録されるべくしてされたものであることを確認し、そのストレージメディアそのものでないと再生できないようにする。すなわち、この場合、そのストレージメディアから、別のストレージメディア（例えば別のDVD-RAM）にコピー（デジタルダビング）を行なった場合には、コピーメディアでは再生ができないようにする。

【0153】そのために、受信装置102からMPEG4配信サーバ101に、受信装置102で用いるストレージメディアのID（通し番号）MIDを通知し（ステップS7203）、MPEG4配信サーバ101では、このMIDの値を用いて暗号鍵Kcを暗号化して、受信装置102に通知する（ステップS7204）。より具体的には、予め定められた関数gを用いて $W = g(MID)$ の形で暗号鍵Wを生成し、この暗号鍵Wを用いて暗号鍵Kcを暗号化し（この暗号鍵Wで暗号化された暗号鍵Kcを $[Kc]w$ と記述する）、 $[Kc]w$ を送信する。ここで、MIDの値は、ストレージメディア毎に異なる値であるとし、ROM等の書き換え不可能な領域に持っているものとする。

【0154】上記の $[Kc]w$ を受信した受信装置102は、MPEG4配信サーバ101と同一の関数gを用いて $W = g(MID)$ の形で暗号鍵Wを生成し、この暗号鍵Wを用いて $[Kc]w$ を復号して暗号鍵Kcを求める。

【0155】以降は、MPEG4配信サーバ101では、AVデータからMPEG4データを生成し、上記のようにして共有された暗号鍵KcでこのMPEG4データを暗号化し、暗号化MPEG4データを、AVデータが受信装置102に対して送信する（ステップS7206）。

【0156】一方、受信装置102は、受信した暗号化された暗号化されたMPEG4データを、上記のようにして求めた暗号鍵Kcで復号し、該MPEG4データをデコードして、AV出力として出力する。

【0157】また、本実施形態では、受信装置102は、AVデータ（暗号鍵Kcで暗号化されたMPEG4データ）を受信すると同時にもしくは一旦バッファ等に蓄積した後に、受信したAVデータを暗号鍵Kcで暗号化されたMPEG4データの形で、 $[Kc]w$ の値とともに、先のMIDを持つストレージメディアに記録する機能を有する。

【0158】この場合、この適正なストレージメディアに記録されたAVデータ（暗号鍵Kcで暗号化されたMPEG4データ）を再生する装置（受信装置102であってもよいし、他の装置であってもよい）は、まず、該ストレージメディアから $[Kc]w$ の値およびMIDを読み出し、 $W = g(MID)$ の形で暗号鍵Wを生成し、

この暗号鍵Wで $[Kc]w$ を復号して暗号鍵Kcを求める。そして、ストレージメディアに記録されたAVデータ（暗号鍵Kcで暗号化されたMPEG4データ）を読み出して、この暗号鍵Kcで復号した後にMPEG4データをデコードする。

【0159】一方、あるMID1を持つストレージメディアに記録されたAVデータ（暗号鍵Kcで暗号化されたMPEG4データ）を、異なるMID2を持つストレージメディアにコピーした場合、このコピー先のストレージメディアに記録されたデータを再生する装置においては、もとの適正なストレージメディアのMIDが得られないので、Wを生成できず、よって記録されている

$[Kc]w$ から暗号鍵Kcを求めることができず、この結果、記録された暗号化データを復号することができないことになる。すなわち、適正なKc、W、 $[Kc]w$ を、 $Kc1$ 、 $W1 = g(MID1)$ 、 $[Kc]w1$ とすると、該ストレージメディアから読み出したMIDはMID2であり、これをもとに生成した暗号鍵Wは、 $W2 = g(MID2)$ となるので、該ストレージメディアから読み出した $[Kc]w1$ をW2で復号すると、Kcとは異なる値が求まる（これをKc'とする）。したがって、Kcで暗号化されたデータ $[Data]Kc$ をKc'で復号しても、もとのデータDataとは異なるData'が生成され、もとのデータDataを得ることはできない。

【0160】このように、受信したAVデータ（暗号鍵Kcで暗号化されたMPEG4データ）を他のストレージメディアメディアにコピーしても、そのストレージメディアのMIDの値が異なるため、当該AVデータを再生不能とすることができ、不正な複製を未然に防止することができる。

【0161】なお、本実施形態において、RTPヘッダ、暗号拡張（バイロード）ヘッダ、MPEG4拡張（バイロード）ヘッダ等に関しては、第1～第7の実施形態と同様の構成でよい。

【0162】以上の各実施形態では符号化方式としてMPEG4を例にとって説明したが、もちろん他の符号化方式も使用可能である。この場合には、各実施形態の装置の該当する構成部分（例えば、MPEG4データ生成部、MPEG4拡張ヘッダ付与部、MPEG4データデコード部、MPEG4拡張ヘッダ受信解析部等）、拡張ヘッダ（MPEG4拡張ヘッダ、MPEG4バイロードヘッダ）、バイロードタイプの記述等を、それぞれの符号化方式に応じて修正すればよい。また、各実施形態の配信サーバは、必要に応じて、コンテンツを暗号化しないで送信するようにすることも可能である。すなわち、暗号化の有無に応じて、暗号化有無フィールドやバイロードタイプ等の記述内容を適宜決定すればよい。受信装置側も、受信したパケットのヘッダから暗号化の有無を調べることにより、暗号化の有無に応じて復号化処理を

制御すればよい。

【0163】なお、以上の各機能は、ソフトウェアとしても実現可能である。

【0164】また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【0165】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0166】

【発明の効果】本発明によれば、コピープロテクション技術をIEEE1394のみならずインターネット等のネットワーク上のコンテンツ流通にも拡張することが可能となる。

【図面の簡単な説明】

【図1】本発明の第1～第6の実施形態に係るネットワークの構成例を示す図

【図2】本発明の第1～第6の実施形態に係るシーケンスの例を示す図

【図3】本発明の第1の実施形態に係るMPEG配信サーバの構成例を示す図

【図4】暗号拡張ヘッダのフォーマットの第1の例を示す図

【図5】RTP処理部で付与されるヘッダのフォーマットの第1の例を示す図

【図6】転送されるIPパケットのフォーマットの第1の例を示す図

【図7】本発明の第1の実施形態に係る受信装置の構成例を示す図

【図8】本発明の第2、第3、第5の実施形態に係るMPEG配信サーバの構成例を示す図

【図9】RTP処理部で付与されるヘッダのフォーマットの第2の例を示す図

【図10】転送されるIPパケットのフォーマットの第2の例を示す図

【図11】本発明の第2、第3、第5の実施形態に係る受信装置の構成例を示す図

【図12】RTP処理部で付与されるヘッダのフォーマットの第3の例を示す図

【図13】転送されるIPパケットのフォーマットの第3の例を示す図

【図14】本発明の第4、第6の実施形態に係るMPEG配信サーバの構成例を示す図

【図15】RTP処理部で付与されるヘッダのフォーマットの第4の例を示す図

【図16】転送されるIPパケットのフォーマットの第4の例を示す図

【図17】本発明の第4、第6の実施形態に係る受信装置の構成例を示す図

【図18】RTP処理部で付与されるヘッダのフォーマットの第5の例を示す図

【図19】暗号拡張ヘッダのフォーマットの第2の例を示す図

【図20】転送されるIPパケットのフォーマットの第5の例を示す図

【図21】RTP処理部で付与されるヘッダのフォーマットの第6の例を示す図

【図22】転送されるIPパケットのフォーマットの第6の例を示す図

【図23】本発明の第7の実施形態に係るネットワークの構成例を示す図

【図24】本発明の第7の実施形態に係るシーケンスの例を示す図

【図25】本発明の第7の実施形態に係るMPEG配信サーバの構成例を示す図

【図26】転送されるIPパケットのフォーマットの第7の例を示す図

【図27】RTP処理部で付与されるヘッダのフォーマットの第7の例を示す図

【図28】本発明の第7の実施形態に係る受信装置の構成例を示す図

【図29】本発明の第8の実施形態に係るシーケンスの例を示す図

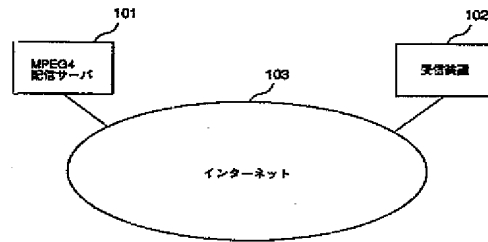
【符号の説明】

101、6101…MPEG4 配信サーバ
102、6102…受信装置
103、6103…インターネット
6104…プロキシサーバ
6105…LAN
301、6301…MPEG4 データ生成部
302、6302…データ暗号部
303、703…RTP処理部
304…暗号拡張ヘッダ付与部
314…暗号ペイロードヘッダ付与部
305…MPEG4 拡張ヘッダ付与部
315、6305…MPEG4 ペイロードヘッダ付与部
306…RTP基本ヘッダ付与部
307…RTCP送信部
308、702、6308、6702…TCP/IP及びUDP/IP処理部
309、701、6309、6701…リンク・物理レイヤ処理部
310…RTCP受信解析部
311、711、6311、6711…認証・鍵交換処理部
704…RTP基本ヘッダ受信解析部
705…MPEG4 拡張ヘッダ受信解析部

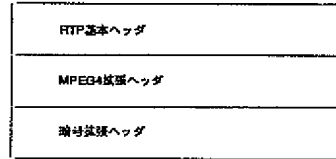
715...MPEG4ペイロードヘッダ受信解析部
706...暗号拡張ヘッダ受信解析部
716...暗号ペイロードヘッダ受信解析部
707, 6707...データ暗号復号部
708, 6708...MPEG4データデコード部
709...受信状態解析部
710...RTCP送信部

6303, 6703...HTTP処理部
6304...暗号ヘッダ付与部
6306...MIMEヘッダ付与部
6704...MIMEヘッダ解析部
6705...MPEG4ペイロードヘッダ解析部
6706...暗号ヘッダ解析部

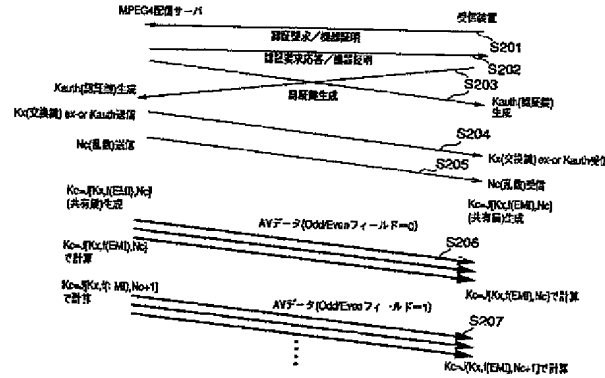
【図1】



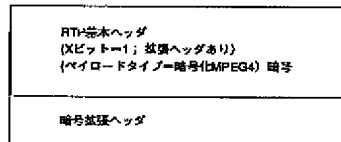
【図5】



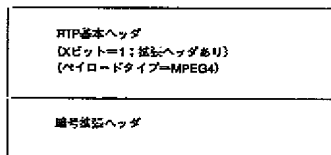
【図2】



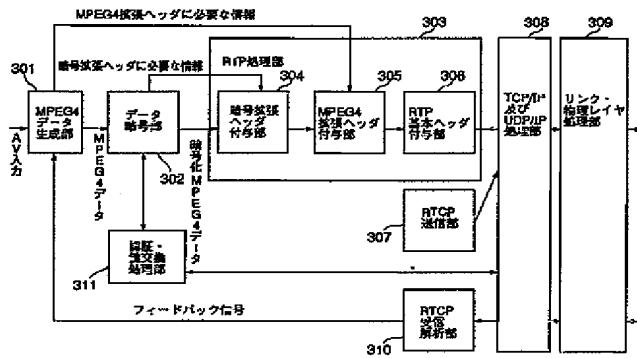
【図9】



【図12】



【図3】



【図4】

	拡張ヘッダ種別フィールド (四ビット符号拡張ヘッダ)
8ビット	符号化有無フィールド (符号あり)
8ビット	符号方式指示フィールド (符号方式=M6)
8ビット	符号モードインジケータ (EMD) フィールド
8ビット	Even/Oddフィールド

【図10】

【図6】

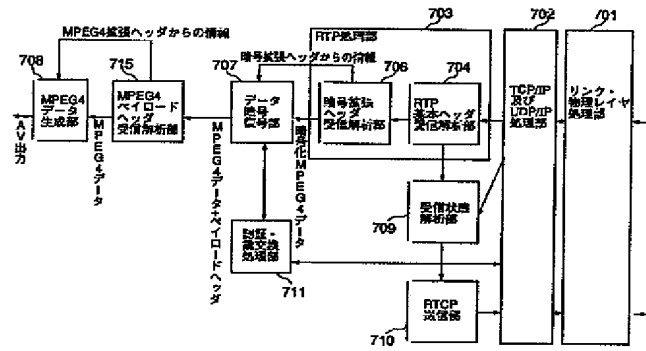
IPヘッダ(IPv4/IPv6)	
UDPヘッダ	
RTPヘッダ	RTP基本ヘッダ
	MPEG4拡張ヘッダ
	符号拡張ヘッダ
MPEG4データPES (符号化されたMPEG4データ)	

【図15】

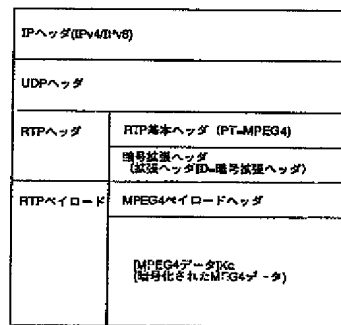
IPヘッダ(IPv4/IPv6)	
UDPヘッダ	
RTPヘッダ	RTP基本ヘッダ (X=符号化MPEG4)
	符号拡張ヘッダ
RTPペイロード	MP: X4ペイロードヘッダ
	MPEG4データPES (符号化されたMPEG4データ)

RTP基本ヘッダ (Xビット=0: 拡張ヘッダ無し) (ペイロードタイプ=符号化MPEG4)
--

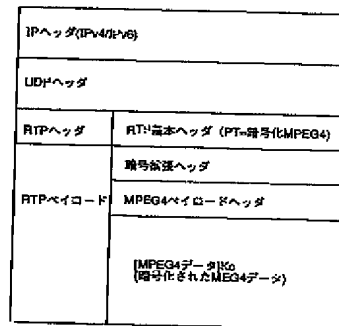
【図11】



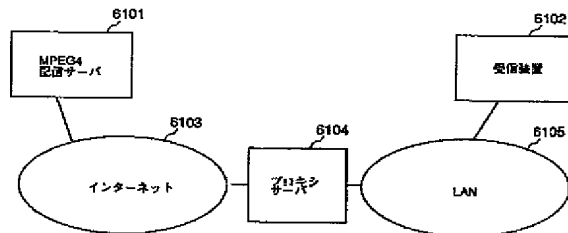
【図13】



【図16】



【図23】



【图 14】



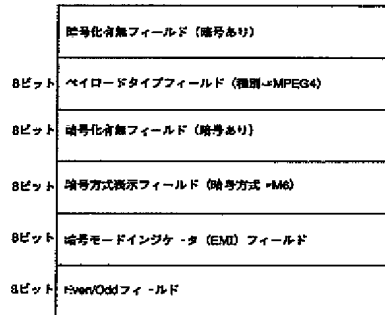
MIME基本ヘッダ

MIME-Version:1.0
Message-ID:User-1
Content-Type:multipart/mixed
boundary="boundary1"

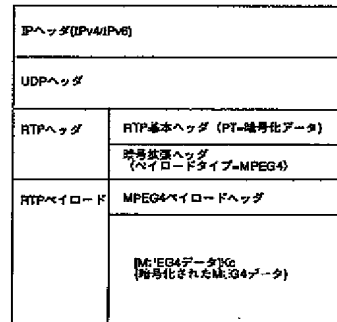
符号拡張ヘッダ

Content-Type:application/x-encryption
符号方式表示フィールド(符号方式=M0)
符号化有無フィールド(符号あり)
符号コードインジケータ(ENI)フィールド
SymbolicName:Symbol

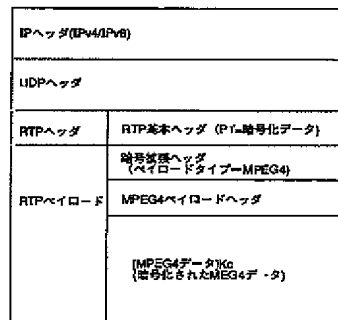
【図19】



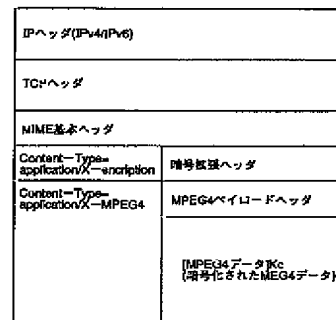
【図20】



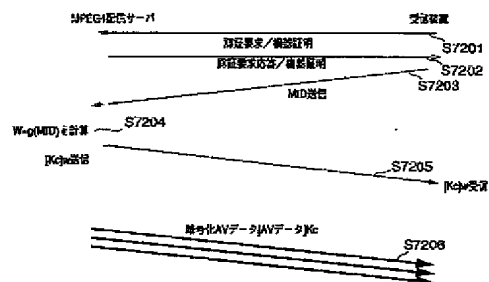
【図22】



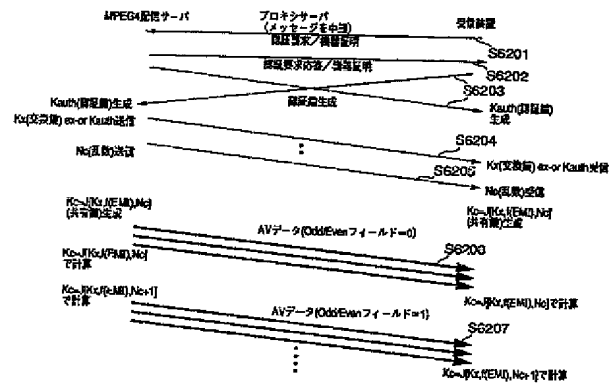
【図26】



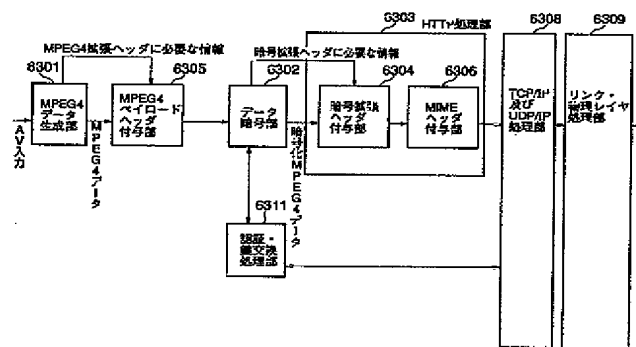
【図29】



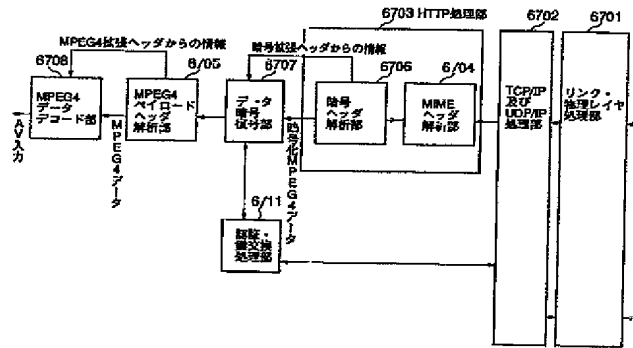
【図24】



【図25】



【図28】



フロントページの続き

(72)発明者 友田 一郎
神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内
(72)発明者 高島 由彰
神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内
(72)発明者 網 淳子
神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

Fターム(参考) 5C064 CA14 CB01 CC04
5J104 AA07 KA01 KA02 KA04 MA07
PA07
5K030 GA15 HA08 HB11 HB16 HB21
JA05 KA01 KA06 LA07 LD19
LD20
9A001 BB04 CC04 CZ06 DD10 EE01
EE04 EZ03 HZ27 JJ18 JJ19
JZ25 LL03